[ORAL ARGUMENT SCHEDULED FOR MAY 8, 2019]

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER, *Appellant*, v. UNITED STATES DEPARTMENT OF COMMERCE, et al., *Appellees*.	Case No. 19-5031

APPELLANT'S RESPONSE ADDRESSING THE STATUS OF THIS APPEAL

Appellant Electronic Privacy Information Center ("EPIC") hereby submits this response to the Court's May 6, 2019 Order concerning the status of this appeal.

This remains a live appeal. The Government has yet to complete the privacy impact assessments required by section 208 of the E-Government Act. The brief modification to an earlier assessment, provided by the agency late on Friday afternoon, is post hoc, incomplete, and cursory and fails to address the required elements of a privacy impact assessment set out by Congress in section 208. Most significantly, there is no indication that the

May 2, 2019 filing played any role in the Secretary's decision to collect personal data regarding citizenship status in the decennial census. Thus, the central purpose of section 208—that the privacy impact assessments be conducted, reviewed, and published "before . . . initiating a new collection of information"—was not fulfilled. E-Government Act § 208(b)(1)(A).

Accordingly, this case should proceed to oral argument as scheduled, and the Court should enter a preliminary injunction halting the Census Bureau's collection of personal data concerning citizenship status at least until adequate assessments are completed.

The Government's eleventh-hour filing does not change the status of this case. The document submitted by the Government—which merely adds two brief paragraphs to an existing document—falls well short of the "extensive" privacy assessments that section 208 requires. OMB Guidance § II.C.2.a.ii, ADD 34. The Government has failed to comply with section 208 and the implementing regulations in several respects.

First, the Government's cursory analysis of the collection of citizenship data is not remotely "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information[.]" E-Government Act § 208(b)(2)(B)(i). The decennial census is arguably the most extensive collection of personal data

performed by the federal government, and the collection of citizenship information is the most controversial component of the 2020 Census. The privacy impact of such an undertaking cannot be adequately addressed in a few short sentences.

Second, the Government fails to explain how personal data concerning citizenship status will be "use[d]," "secured," or "shared" once it is transferred from CEN08 to the other CEN systems at issue in this case. E-Government Act §§ 208(b)(2)(B)(ii)(III), (IV), (VI). Thus, even if the Government's two-paragraph analysis were somehow adequate for the purposes of CEN08, it fails to fully account for numerous IT systems used to collect, maintain, and disseminate personal data collected through the census.

Third, even assuming the Government is seeking personal data regarding citizenship status to improve enforcement of the Voting Rights Act, the Government fails to evaluate whether alternative processes for developing block-level citizenship data would "mitigate potential privacy concerns" of collecting of citizenship information via the census. OMB Circular A-130, p. 34, ADD 29; *see also* OMB Guidance § II.C.2.a.ii, ADD 34 (requiring analyses of "the alternatives to collection and handling as designed"; "the appropriate measures to mitigate risks identified for each alternative"; and "the rationale for the final design choice").

Fourth, the Government fails to address whether the proposed use of collected citizenship information would "conform[] to applicable legal, regulatory, and policy requirements regarding privacy," OMB Circular A-130 at p. 34, ADD 29. In particular, the Government does not explain whether the planned use of the personal data is consistent with the Bureau's policy governing the provision of census data to other agencies. *See* U.S. Census Bureau, *DS-021, Policy on Providing Custom Tabulations and Custom Extracts Under 13 U.S.C. § 8(b)* (Aug. 20, 2015).[1]

Fifth, the Government represents that "only deidentified statistical information" will be transferred to the Department of Justice. U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN08 Decennial Information Technology Division (DITD)* (approved May 2, 2019). However, the Government fails to describe what techniques will be used to ensure that the data will remain deidentified. Data that is today deidentified could, following the development of new techniques, be later transformed into personally identifiable information. As the National Academies has explained, "The proliferation of publicly accessible data, outside of the statistical agencies, has dramatically increased the risks inherent in releasing micro-data because these other data sources can be used to re-identify

[1] https://www2.census.gov/foia/ds_policies/ds021.pdf.

putatively anonymized data." Nat'l Acads. of Scis., Eng'g, and Med., *Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy* 77 (2017).[2] And as the President's Council of Advisors on Science and Technology has stated, "Anonymization is increasingly easily defeated by the very techniques that are being developed for many legitimate applications of big data. In general, as the size and diversity of available data grows, the likelihood of being able to re-identify individuals (that is, re-associate their records with their names) grows substantially." President's Council of Advisors on Sci. and Tech., *Big Data and Privacy: A Technological Perspective* at ix (May 2014).[3]

Finally, the Government offers no evidence that it has considered the privacy risks or incorporated privacy protections before making a final decision to collect personal data about citizenship status. Instead, it has made trivial changes to an existing document to create a post hoc rationale for decision finalized over a year ago.

As a result, the Government has still failed to conduct the privacy impact assessments that section 208 requires of every federal agency **before** initiating a new collection of personally identifiable information.

---

[2] https://doi.org/10.17226/24652.

[3] https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

EPIC is therefore entitled to a preliminary injunction halting the Census Bureau's collection of personal citizenship data. Accordingly, this appeal is not moot and should move forward as scheduled. *Cf. Bayala v. United States Dep't of Homeland Sec., Office of Gen. Counsel*, 827 F.3d 31, 34 (D.C. Cir. 2016) ("[T]he entire FOIA case is not moot because [the plaintiff] has not received all of the documents that he requested.").

Respectfully Submitted,

Dated: May 6, 2019

MARC ROTENBERG
EPIC President

ALAN BUTLER
EPIC Senior Counsel

/s/ John L. Davisson
JOHN L. DAVISSON
EPIC Counsel

Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
davisson@epic.org

CERTIFICATE OF SERVICE

I, John Davisson, hereby certify that on May 6, 2019, I electronically filed the foregoing document with the Clerk of the Court for the United States Court of Appeals for the D.C. Circuit by using the CM/ECF system. The following participants in the case who are registered CM/ECF users will be served by the CM/ECF system:

Sarah Carroll
Email: sarah.w.carroll@usdoj.gov
[COR LD NTC Gvt US DOJ]
U.S. Department of Justice
(DOJ) Civil Division, Appellate Staff
Firm: 202-514-2000
950 Pennsylvania Avenue, NW
Washington, DC 20530

Mark B. Stern, Attorney
Email: mark.stern@usdoj.gov
[COR LD NTC Gvt US DOJ]
U.S. Department of Justice
(DOJ) Civil Division, Appellate Staff
Firm: 202-514-2000
950 Pennsylvania Avenue, NW
Washington, DC 20530

/s/ John L. Davisson
JOHN L. DAVISSON

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6). The brief is composed in a 14-point proportional typeface, Times New Roman. The brief also complies with the 1,300-word limit established by this Court's May 6, 2019 order because it contains 975 words.

/s/ John L. Davisson
JOHN L. DAVISSON